UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,428	04/05/2006	Olivier Brique	90500-000035/US	2506

30593 7590 07/12/2010

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
07/12/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/517,428	**Applicant(s)** BRIQUE ET AL.	
	Examiner BRYAN WRIGHT	**Art Unit** 2431	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 07 June 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *17-35*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Note Below:.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Syed Zia/
Primary Examiner, Art Unit 2431

Note: With regards to applicant's remarks of, "…none of the references teach or fairly suggest any "data exchange method between devices locally connected to one another a first device of the two devices being a security module and a second device of the two devices being a receiver," the Examiner contends applicant's paragraph 31 provides the following support for applicant's "connection" claim limitation element: "[0031] The receiver 11, in particular in the case of paying TV, is generally formed by a box connected to the television set". The Examiner respectfully submits Kupka teaches on page 6, lines 25-29 dedicated communication lines between communicating devices. Additionally, Hardy teaches dedicated lines. See Hardy column 4, lines 20-25.

With regards to applicant's remarks of "claim 17 recites the first encrypting key initialized in the first device during an initialization phase of the first device in a first protected environment", the Examiner contends Kupka teaches generating (e.g., initializing) key data within a client system (e.g., protective environment). See Kupka page 13, lines 10-15. Applicant's protective environment is a device.

With regards to applicant's remarks of "Acknowledging the deficiencies of Hardy and Kupka in teaching each and every limitation of independent claim 17, the Examiner relies on the teachings of Takahashi to teach "the second encrypting key initialized in the second device during an initialization phase of the second device in a second protected environment," as recited in independent claim 17", the Examiner contends Kupka teaches a asymmetric encryption scheme in which one device maintains a public key for encrypting the data and another device maintains a private key for decrypting the data. Kupka states that the private key is only held by one person and the public key can be held by anyone. Kupka describes this encryption scheme for encrypting and decrypting data sent between a server and a client. In this instance, the server would hold the public key and client would hold the private key. Therefore, this would suggest to one ordinary skill in the art that the private key will be initialized and held only at the client device. See Kupka page 10, lines 15-23. The Examiner contends that prior reference Takahashi performs a similar encryption scheme.

With regards to applicant's remarks of "Accordingly the sacred keys of Takahashi cannot facilitate and/or be used for communication between "two devices locally connected to one another, a first device of the two devices being a security module and a second device of the two devices being a receiver, as required by claim 17", the Examiner contends that semantically a device can be reference in any manner, (e.g., receiving device, security module), however the applicant does not provide any argument that would suggest that the device of Takahashi is different hardware wise.

With regards to applicant's remarks of "It is alleged in the Office Action at page 4 that Hardy teaches "a session key" as required by independent claim 17. Particularly, the Examiner alleges that Hardy teaches combining of first and second random numbers to form a third random number. In Hardy, the third random number is used as a traffic key for the selected key generator for both terminals. However, Hardy does not disclose or even suggest that the traffic key is used as a "session key" as required by independent claim 17", the Examiner contends that the term "session key" is commonly associated with key data that is used in the art to facilitate communication between communicating device. Hardy discloses encrypting and decrypting communication data with key data (e.g., session key) in column 4, lines 50-55. Additionally, Takahashi expreslsy dislcoses the use of "session key".

With regards to applicant's remarks of "Column 2, Line 41 of Takahashi discloses a cryptographic technique that uses a session key to encrypt communication. However, nothing in Takahashi discloses or even fairly suggests that this session key of Takahashi is generated by "combining a first and second random number," as required by independent claim 17. For at least this reason Applicants submit that Takahashi fails to disclose or fairly suggest "session key as required by independent claim 17", the Examiner contends Hardy specifically states the use of random numbers in combination to facilitate secure communication exchange. See Hardy column 6, lines 44-45

With regards to applicant's remarks of "With respect to the Applicant's previously filed amendment, the Examiner alleges on page 11 of the Office Action that the abstract of Hardy discloses "using the session key to encrypt and decrypt all or part of the exchanged data between the first and second device," as required by independent claim 17. However, the traffic keys are only used to initialize key generators. Hardy is silent with regards to any encrypting or decrypting of data exchanged between the first and second devices", the Examiner contends Hardy discloses encrypting and decrypting communication data with key data in column 4, lines 50-55.